格上基于身份的可问责代理重加密方案 *

孟 慧†，任利娜，李 英

(河南理工大学 计算机科学与技术学院，河南 焦作 454003)

摘 要：针对目前基于格的代理重加密方案中存在密钥滥用和数字证书管理等问题，引入问责机制，提出一种新的基于身份的可问责代理重加密方案。该方案采用用户身份 ID 计算生成矩阵作为公钥，并使用原像采样算法提取私钥，解决了数字证书管理的问题；使用双方用户公钥计算生成重密钥，提高了加解密时的计算效率；使用代理商公私钥参与重加密运算，完成问责算法，有效地抑制了代理商和被授权者共谋的行为。安全性分析表明方案满足选择明文攻击安全；在效率方面，方案的计算复杂度和密文开销较小。

关键词：代理重加密；格密码；带错误学习问题；可问责性

中图分类号：TP309 doi: 10.19734/j.issn.1001-3695.2021.12.0693

Identity-based accountable proxy re-encryption scheme from lattice

Meng Hui†, Ren Lina, Li Ying

(*School of Computer Science & Technology*, *Henan Polytechnic University*, *Jiaozuo Henan* 454003, *China*)

Abstract: Aiming at the problems of key abuse and digital certificate management in the current lattice-based proxy re-encryption scheme, this paper proposed a new identity based accountable proxy re encryption scheme by introducing the accountability algorithm. This scheme used the user ID to calculate matrix as the public key and used the pre-image sampling algorithm to extract the private key, which solved the problem of digital certificate management; used the public keys of both users to calculate and generate the re-encryption key, which improved the computational efficiency of encryption and decryption; used the proxy's public and private keys to participate in the re-encryption calculation, completed the accountability algorithm, and inhibited the collusion of the proxy and the delegatee. The security analysis shows that the scheme satisfies the chosen-plaintext attack security. In terms of efficiency, the scheme has less computational complexity and ciphertext overhead.

Key words: proxy re-encryption; lattice; learning with error; accountability

0 引言

目前，云存储和云端数据共享在网络数据存储与计算中占据核心地位，用户将大量的数据存储在网络云盘中，减轻自己存储设备的负担，同时，更利于用户之间共享数据。在复杂的网络环境中，用户为了保护数据隐私需要将数据加密后再上传至云服务器存储或共享，但是，数据发送者需要实时查看是否有用户访问数据，并将要访问的数据下载后转发给数据接收方。代理重加密解决了传统云计算环境中数据拥有者需要实时在线的问题，减轻了用户频繁访问云端密文数据的负担，增强了数据的可靠性和机密性。1998 年，Blaze 等人[1]首次提出了代理重加密(Proxy Re-encryption，PRE)的概念，在公钥加密系统中加入代理商的角色，并由代理商使用重密钥完成密文转换。2007 年，Green 等人[2]第一次提出了基于身份的代理重加密(IB-PRE)方案，方案中，公钥直接使用用户身份 ID，公钥基础设施中的证书管理问题得到解决，该方案满足多跳性和非交互性。然而，随着量子计算机的发展，传统数论难题的安全性受到威胁。2010 年，Xagawa 等人[3]首次提出了格上的代理重加密方案，该方案不仅可以能够抵抗量子攻击还降低了计算复杂度。2014 年，Singh 等人[4]将身份基和代理重加密融合，提出了一个可以加密多比特信息的 PRE 方案，提高了运算效率。而且所提方案满足匿名性、多跳性。2021 年，汤永利等人[5]利用 RLWE (Ring Learning With Errors)难题构造了一个 PRE 方案，有效缩短了密文、密钥尺寸，提高了加解密的效率。但是，以上几种方案都具有双向性，不能抵抗合谋攻击，且存在密钥泄漏等安全问题。2016 年，Kim[6]等人提出了第一个基于最坏情况的格上难题且满足单向性的代理重加密方案，方案中的被授权者无法感知代理商的存在，即使用重密钥加密的密文和使用被授权方公钥加密的密文是不能被区分的。2020 年，wang[7]等人指出了 Kim 方案中重加密密文无法解密或解密错误率高的问题，提出了一个新的满足单向性的代理重加密方案，经证明方案满足选择明文攻击(Chosen-plaintext Attack，CPA)安全。2021 年，Dutta 等人[8]提出第一个针对选择性和自适应身份的抗合谋单向 IB-PRE 的具体构造，所提结构具有非交互性和非传递性，不满足多跳性。

2013 年，Wang 等人[9]提出了一个新的原语 PRE$^+$，与传统 PRE 的不同点在于解密权的委托者不同。传统 PRE 解密权限的委托者是密文接收方，而 PRE$^+$解密权限的委托者是密文发送者，即加密者将解密权委托给被授权者。且重密钥生成算法中的输入元素不同，传统 PRE 由密文接收方的私钥与被授权者的私钥或公钥生成重密钥，而 PRE$^+$是由两者的公钥生成重密钥。2020 年，Singh 等人[10]提出了单向的 PRE 和 PRE$^+$方案，PRE$^+$能够提高加解密时的计算效率，适用于细粒度授权和不可转让授权，在安全云计算和组播等方面应用广泛。被授权者和代理商的合谋攻击虽

收稿日期：2021-12-01；**修回日期：**2022-02-14 **基金项目：**国家自然科学基金资助项目(61802117)；河南省高校科技创新团队项目(20IRTSTHN013)；河南省高等学校重点科研项目(19A520024)；河南理工大学博士基金资助项目(B2013-037)

作者简介：孟慧(1981-)，女(通信作者)，河南焦作人，讲师，硕导，博士，主要研究方向为网络信息安全(menghui@hpu.edu.cn)；任利娜(1998-)，女，河南濮阳人，硕士研究生，主要研究方向为网络与信息安全；李英(1998-)，女，河南南阳人，硕士研究生，主要研究方向为网络与信息安全.

然不会暴露授权者的长期密钥，但是，他们可能会合谋并为不受委托方信任的恶意用户提供新的重密钥。另外，由于代理重加密的固有功能可能会使 PRE 方案存在重密钥滥用问题，即代理商和被授权者合谋获得授权者的解密能力，并将其保存在任何载体上，如解密设备。为了缓解这个问题，2005 年，Ateniese 等人[11]提出不可转让的概念，当 Bob 和代理商合谋分发 Alice 的解密能力时，Bob 必须公开他自己的解密能力作为代价。2019 年，Guo 等人[12]使用不可区分性混淆和 K-不可伪造认证构造了不可转让的代理重加密方案。不可转让性对恶意用户有一定的威慑作用，但是，当 Bob 的密钥远没有数据拥有者的密钥有价值时，Bob 可能会为了更大的利益而公开自己的解密能力。此时代理商可以从中分发 Alice 的解密能力，却不用付出任何代价，甚至否认自己的恶意行为。2021 年，Guo 等人[13]为了解决上述问题提出了可问责的代理重加密(Accountable Proxy Re-encryption，APRE)方案，并引入一个判断算法来判断代理商是否不承认自己分发授权者解密能力的行为。可问责代理重加密模型如图 1 所示。

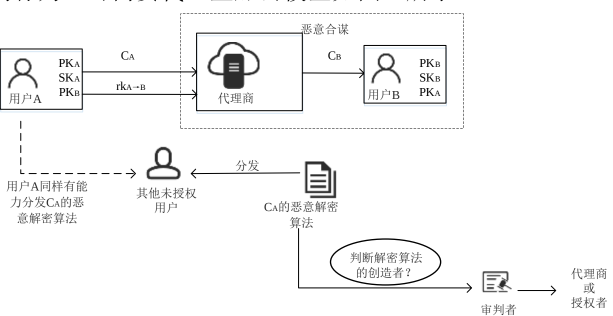


图 1　可问责代理重加密模型

Fig. 1　Accountable proxy re-encryption model

为了解决公钥加密中的数字证书管理和密钥滥用等问题，基于文献[13]中的问责算法构造一个新的格上基于身份的可问责代理重加密方案。利用用户身份 ID 计算生成一个矩阵作为公钥，取代传统公钥加密体制中将用户身份和公钥联系起来的数字证书，使用原像采样算法提取私钥，并且令代理商公私钥参与重密钥和重加密的计算，最后，使用一个公开的审判算法判断恶意代理是否在否认自己分发授权者解密能力的行为。与文献[13]不同的是，本文方案基于带错误学习(Learning with Error，LWE)困难假设，使用用户身份作为公钥并使用授权者公钥参与重密钥的运算。安全分析表明，方案在标准模型下达到适应性选择身份的选择明文攻击安全下的不可区分性(IND-aID-CPA)。效率分析则说明方案在存储空间、性能和复杂度上的优势。

1　预备知识

1.1　格

设 $\boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n\}$ 是由 $\mathbb{R}^m$ 中 n 个向量组成的矩阵，且这些向量是线性无关的，则这 n 个向量的所有整系数的线性组合所构成的集合为一个 m 维格 Λ，即：

$$\Lambda=\mathcal{L}(\boldsymbol{B})=\{\boldsymbol{y}\in\mathbb{R}^m, s.t.\exists \boldsymbol{s}\in\mathbb{Z}^n, \boldsymbol{y}=\boldsymbol{Bs}=\sum_{i=1}^{n}s_i\boldsymbol{b}_i\}$$

其中：$\boldsymbol{b}_1,\boldsymbol{b}_2,\ldots,\boldsymbol{b}_n$ 是格 Λ 的一组基，当 $m=n$ 时，称格 Λ 是满秩格。

定义 1　设 q 为素数，矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，定义两个 m 维满秩整数格：

$$\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{e}\in\mathbb{Z}^m, s.t. \boldsymbol{Ae}=\boldsymbol{0}(\mathrm{mod}\, q)\}$$

$$\Lambda_q(\boldsymbol{A})=\{\boldsymbol{y}\in\mathbb{Z}^m, s.t.\exists \boldsymbol{s}\in\mathbb{Z}_q^n, \boldsymbol{A}^T\boldsymbol{s}=\boldsymbol{y}(\mathrm{mod}\, q)\}$$

格上的陷门函数在格密码学中有着广泛的应用，陷门基是格的一个短基，方案中使用陷门生成算法产生的陷门基作为主私钥。

引理 1[14]　陷门生成算法：整数 $q\geq 3$，$m=\lceil 6n\log q\rceil$。存在一个概率多项式时间(Probabilistic Polynomial-time，PPT)算法 TrapGen(q,n) 生成矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的一组基 $\boldsymbol{T}\in\mathbb{Z}_q^{m\times m}$，其中 $\boldsymbol{A}$ 在 $\mathbb{Z}_q^{n\times m}$ 上的分布与均匀分布是不可区分的，且 $\|\tilde{\boldsymbol{T}}\|\leq O(\sqrt{n\log q})$ 和 $\|\boldsymbol{T}\|\leq O(n\log q)$ 以绝对的优势成立。

1.2　离散高斯分布

高斯分布常用于格上困难问题的研究，本节将对离散高斯分布和其相关引理作出详细介绍。

对于 $\forall s\in\mathbb{R}_+$，$c\in\mathbb{R}^m$，定义 m 维格 Λ 上的离散高斯分布：

$$D_{\Lambda,s,c}(\boldsymbol{x})=\frac{\rho_{s,c}(\boldsymbol{x})}{\rho_{s,c}(\Lambda)}=\frac{\rho_{s,c}(\boldsymbol{x})}{\sum_{x\in\Lambda}\rho_{s,c}(\boldsymbol{x})}$$

文献[14]中介绍了原像采样算法，其中包含的 SamplePre 算法负责使用陷门基 $\boldsymbol{T_A}$ 求解给定像值 $\boldsymbol{u}$ 对应的原像值 $\boldsymbol{x}$。

引理 2[14]　SamplePre$(\boldsymbol{A},\boldsymbol{T_A},\sigma,\boldsymbol{u})$ 已知格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 上的一个陷门基 $\boldsymbol{T_A}$，实数 $\sigma\geq\|\tilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\omega(\sqrt{\log n})$，对于任意向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，存在一个 PPT 算法 SamplePre$(\boldsymbol{A},\boldsymbol{T_A},\sigma,\boldsymbol{u})$，在统计量接近 $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}),\sigma,c}(\boldsymbol{x})$ 的分布中抽取一个向量 $\boldsymbol{x}\in\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})$，满足 $\boldsymbol{Ax}=\boldsymbol{u}(\mathrm{mod}\, q)$。

引理 3[15]　设正整数 n，q，其中 q 为素数，$m\geq 2n\log_2 q$。那么对于 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，$\sigma\geq\omega(\sqrt{\log_2 m})$，$\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,\sigma}$，$\boldsymbol{u}=\boldsymbol{Ae}\,\mathrm{mod}\, q$ 的分布与 $\mathbb{Z}_q^n$ 上的均匀分布的统计量相近。

1.3　格上困难问题

定义 2[16]　小整数解问题 SIS。给定素数 $q>0$，随机选择矩阵 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$，找到一个非零向量 $\boldsymbol{u}\in\mathbb{Z}_q^m$，使 $\boldsymbol{Bu}=\boldsymbol{0}\,\mathrm{mod}\, q$，并且满足 $\|\boldsymbol{u}\|\leq\delta$，其中，常数 $\delta>0$。

文献[17]给出从最坏情况困难到 SIS 的归约，证明 SIS 问题在某些参数下是足够困难的。

定理 1[17]　设整数 $n\geq 1$，$m=poly(n)$ 和实数 $\beta\geq\beta_\infty\geq 1$，令 $\boldsymbol{Z}^*=\{\boldsymbol{z}\in\mathbb{Z}^m:\|\boldsymbol{z}\|_2\leq\beta,\|\boldsymbol{z}\|_\infty\leq\beta_\infty\}$ 并且 $q\geq\beta n^\delta$，常数 $\delta>0$。则求解解集为 $\boldsymbol{Z}^*\backslash\{0\}$ 的 $SIS_{m,n,q,\delta}$ 问题至少与在 n 维格上将最坏情况下的格问题逼近到 $\max\{1,\beta\cdot\beta_\infty/q\}\cdot\tilde{O}(\beta\sqrt{n})$ 一样困难。

定义 3[18]　带错误学习问题 LWE。给定正整数 n 和 q，选择均匀随机的矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$，向量 $\boldsymbol{e}\leftarrow\chi^m$ 服从错误分布。LWE 困难问题就是给定 $(\boldsymbol{A},\boldsymbol{A}^T\boldsymbol{s}+\boldsymbol{e})$，以不可忽略的概率寻找 s。

定义 4[4]　$\mathrm{LWE}_{q,\chi}$ 判定问题 DLWE。设正整数 n，m 以及素数 q，χ^m 是 $\mathbb{Z}_q$ 上的高斯分布。LWE 的判定性问题是指通过随机给出一系列来自分布 $A_{s,\chi}$ 的独立抽样或者来自 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 的均匀随机抽样，判断抽样是否来自分布 $A_{s,\chi}$ 的问题。

文献[18]中给出了 LWE 和 DLWE 的关系以及从最短向量问题(SVP)到 LWE 的归约，证明 LWE 对于某些参数是足够困难的。

定理 2[18]　n,q 为正整数，实数 $\alpha\in(0,1)$，满足 $\alpha q>\sqrt{2n}$。若 LWE 问题能被一个有效的算法解决，那么近似决策性最短向量问题(Gap-SVP)和最短独立向量问题(SIVP)的最坏情况问题也能够被一个量子算法以 $\tilde{O}(n/\alpha)$ 的时间复杂度解决。

2　可问责代理重加密定义及安全模型

2.1　可问责代理重加密的定义

下面是对身份基可问责代理重加密定义的介绍，安全参数为 λ。

(1)初始化 Setup(λ)：输入安全参数 λ，输出公共参数 $params$ 和主私钥 msk；

(2)私钥提取 Extract$(params,msk,id)$：输入 $params$，msk 和用户 id，输出用户私钥 SK；

(3)加密 Enc$(params,id_i,m)$：输入 id_i 和明文 m，输出二级密文 C_i；

(4)重密钥生成 ReKeyGen$(params,id_i,id_j,id_p)$：以公共参数 $params$ 和双方用户及代理商的身份 id 作为输入，输出重密钥 $rk_{i\to j}$；

(5)重加密 $\text{ReEnc}(params, rk_{i\to j}, SK_p, C_i)$：输入 $rk_{i\to j}$，代理商私钥 SK_p 和 C_i，输出一级密文 C_j；

(6)二级密文解密 $\text{Dec}_2(params, SK_i, C_i)$：输入 SK_i 和二级密文 C_i，算法解密恢复出明文 m；

(7)一级密文解密 $\text{Dec}_1(params, SK_j, C_j)$：输入 SK_j 和一级密文 C_j，输出明文 m；

(8)问责算法 $\text{Judge}^{D_{i,\mu}}(params, id_i, id_p)$：通过黑盒访问解密设备 $D_{i,\mu}$，id_i 和 id_p 作为输入，该算法输出 Proxy 或 Delegator，输出结果即为恶意解密设备的生成者。

正确性：方案满足以下两个条件，即可正确恢复明文。

$$\text{Dec}_2(params, SK_i, \text{Enc}(params, id_i, m)) = m\text{；}$$

$$\text{Dec}_1(params, SK_j, \text{ReEnc}(params, rk_{i\to j}, SK_P, \text{Enc}(params,\ id_i, m))) = m$$

2.2　可问责代理重加密的安全模型

2.2.1 CPA 安全

本小节将介绍基于 IND-aID-CPA 游戏的可问责代理重加密安全模型[19]，设安全参数为 λ，游戏是由敌手$\mathcal{A}$和下列预言机组成，过程如下：

初始化阶段：挑战者$\mathcal{C}$将 $\text{Setup}(\lambda)$ 输出的公共参数 $params$ 发送给敌手$\mathcal{A}$。

阶段 1：敌手$\mathcal{A}$发出问询，挑战者$\mathcal{C}$作出回答：

私钥生成预言机 O_{SK}：使用 $\text{Extract}(params, msk, id_i)$ 生成用户私钥 SK_i 并存储，当敌手$\mathcal{A}$输入 id_i 时，若用户 i 为恶意用户，则挑战者$\mathcal{C}$发送 SK_i 给敌手$\mathcal{A}$。否则，发送⊥；

重密钥生成预言机 O_{rk}：敌手$\mathcal{A}$输入 (id_i, id_j, id_p)，得到 ReKeyGen 生成的重密钥 $rk_{i\to j}$；

重加密预言机 O_{re}：如果用户 j 是不诚实的，则敌手$\mathcal{A}$输入 $(rk_{i\to j}, SK_p, C_i)$，并输出⊥；否则，输出重加密后的密文 $C_j = \text{ReEnc}(\text{ReKeyGen}(id_i, id_j, id_p), SK_p, C_i)$；

挑战预言机 O_C：敌手$\mathcal{A}$输入一个目标用户和两个消息 m_0, m_1。预言机随机选择 $b \in \{0,1\}$，返回挑战者密文 $C^* = \text{Enc}(id^*, m_b)$。

猜测：输入 $b' \in \{0,1\}$，如果 $b' = b$，则挑战者$\mathcal{C}$输出 1，否则输出 0。

定义 5　IND-CPA 安全。定义敌手$\mathcal{A}$的优势为

$$\text{ADV}_{\text{PRE},\mathcal{A}}^{\text{IND-CPA}}(n) = |\Pr[\text{Exp}_{\text{PRE},\mathcal{A}}^{\text{IND-CPA}}(n) = 1] - \frac{1}{2}|$$

当 $\text{ADV}_{\text{PRE},\mathcal{A}}^{\text{IND-CPA}}(n)$ 是可忽略的，称方案是 IND-CPA 安全的。

2.2.2 恶意代理安全

若敌手输出的解密设备使审判者相信诚实的授权者有罪，则敌手赢得游戏。实验过程如下[13]：

Experiment $\text{Exp}_{\text{PRE},\mathcal{A}}^{\text{mp}}(n)$

$params \leftarrow \text{Setup}(\lambda)$

$SK_p \leftarrow \text{Extract}(params, id_p)$

$D_{i,\mu} \leftarrow \mathcal{A}^{O_{SK}, O_{rk}}(params, id_p, SK_p)$

Where μ is a non-negligible probability value;

If $\text{Judge}^{D_{i,\mu}}(id^*, id_p) = \text{Delegator}$

Return 1;

else return 0.

定义 6　恶意代理安全。敌手的优势被定义为

$$\text{ADV}_{\text{PRE},\mathcal{A}}^{\text{mp}}(n) = |\Pr[\text{Exp}_{\text{PRE},\mathcal{A}}^{\text{mp}}(n) = 1]|$$

当所有 PPT 敌手$\mathcal{A}$的优势 $\text{ADV}_{\text{PRE},\mathcal{A}}^{\text{mp}}(n)$ 是可忽略的，方案满足恶意代理安全。

2.2.3 恶意授权者安全

根据下面实验，当解密设备 $D_{i,\mu}$ 使审判者相信诚实的代理商有罪，则敌手赢得游戏。

Experiment $\text{Exp}_{\text{PRE},\mathcal{A}}^{\text{md}}(n)$

$params \leftarrow \text{Setup}(\lambda)$

$SK_p \leftarrow \text{Extract}(params, id_p)$

$D_{i,\mu} \leftarrow \mathcal{A}^{O_{SK}, O_{rk}}(params, id_p)$

Where μ is a non-negligible probability value;

If $\text{Judge}^{D_{i,\mu}}(id^*, id_p) = \text{Proxy}$

Return 1;

else return 0.

定义 7　恶意授权者安全。敌手$\mathcal{A}$的优势被定义为

$$\text{ADV}_{\text{PRE},\mathcal{A}}^{\text{md}}(n) = |\Pr[\text{Exp}_{\text{PRE},\mathcal{A}}^{\text{md}}(n) = 1]|$$

当所有 PPT 敌手$\mathcal{A}$的优势 $\text{ADV}_{\text{PRE},\mathcal{A}}^{\text{md}}(n)$ 是可忽略的，称方案是恶意授权者安全的。

如果 PRE 方案同时满足恶意代理安全和恶意授权者安全，则称这个方案满足可问责性。

3　代理重加密方案

3.1　方案构造

本文基于问责算法与 LWE 困难问题，结合代理重加密与基于身份的加密体制，提出格上基于身份的可问责代理重加密方案，方案具体构造如下：

(1)初始化 $\text{Setup}(\lambda)$：λ 为安全参数，随机矩阵 $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ 和陷门基矩阵 $\boldsymbol{T} \in \mathbb{Z}_q^{m\times m}$ 由陷门生成算法 $\text{TrapGen}(q,n)$ 生成，$\|\tilde{\boldsymbol{T}}\| \le O(\sqrt{n\log q})$，陷门函数 $f_{\boldsymbol{A}}(\boldsymbol{x}) = \boldsymbol{A}\boldsymbol{x} \bmod q\ (f: \mathbb{Z}^m \to \mathbb{Z}_q^n)$。随机选择 m+1 个矩阵 $\boldsymbol{U_0}, \boldsymbol{U_1}, \ldots, \boldsymbol{U_m} \in \mathbb{Z}_q^{n\times m}$，且线性无关，则主密钥为 $mpk = (\boldsymbol{A}, \boldsymbol{U_0}, \boldsymbol{U_1}, \ldots, \boldsymbol{U_m})$，主私钥 $msk = \boldsymbol{T}$，公共参数 $params = (m, n, q, mpk)$。

(2)私钥提取 $\text{Extract}(params, msk, id)$：输入公共参数 params，主私钥 msk 和用户/代理身份 $id = \{id_1, id_2, \ldots, id_m\} \in \{0,1\}$，计算 $\boldsymbol{U} = \boldsymbol{U_0} + \sum_{i=1}^{m} id_i \boldsymbol{U}_i = (\boldsymbol{u_1}, \boldsymbol{u_2}, \ldots, \boldsymbol{u_m})$，使用原像采样算法产生一个向量 $\boldsymbol{x_i} \in \mathbb{Z}_q^m$，使其满足 $\boldsymbol{u_i} = \boldsymbol{A}\boldsymbol{x_i} \bmod q$，$\|\boldsymbol{x_i}\| \le \sigma\sqrt{m}$。令 $\boldsymbol{X} = (\boldsymbol{x_1}, \boldsymbol{x_2}, \ldots, \boldsymbol{x_m})$，则 $\boldsymbol{AX} = \boldsymbol{U} \bmod q$，用户/代理私钥 $SK = \boldsymbol{X}$。

(3)加密 $\text{Enc}(params, id_i, m)$：输入用户 i 的身份 id_i 和明文 $m \in \{0,1\}^m$，随机选择向量 $\boldsymbol{s} \in \mathbb{Z}_q^n$，$\boldsymbol{e} \leftarrow \chi^m$；计算 $C_1 = \boldsymbol{U}_i^T\boldsymbol{s} + m\left\lfloor \frac{q}{2} \right\rfloor + \boldsymbol{e}$，$\boldsymbol{y} = \boldsymbol{A}^T\boldsymbol{s} + \boldsymbol{e}$，输出二级密文 $C_i = (C_1, \boldsymbol{y})$。

(4)重密钥生成 $\text{ReKeyGen}(mpk, \boldsymbol{s}, id_i, id_j, id_p)$：输入随机向量 $\boldsymbol{s}$，用户身份 id_i，id_j 和代理商身份 id_p，选择 $\boldsymbol{e_1} \leftarrow \chi^m$，由用户 i 计算重密钥 $rk_{i\to j} = (\boldsymbol{U}_j^T - \boldsymbol{U}_i^T + \boldsymbol{U}_p^T)\boldsymbol{s} + \boldsymbol{e_1}$。

(5)重加密 $\text{ReEnc}(params, rk_{i\to j}, SK_p, C_i)$：输入重密钥 $rk_{i\to j}$，代理商私钥 SK_p 和二级密文 C_i，选择 $\boldsymbol{e_2} \leftarrow \chi^m$，计算 $C_1' = C_1 + rk_{i\to j} - SK_p^T\boldsymbol{y} + \boldsymbol{e_2}$，输出一级密文 $C_j = (C_1', \boldsymbol{y})$。

(6)二级密文解密 $\text{Dec}_2(params, SK_i, C_i)$：输入 SK_i 和二级密文 C_i，计算 $m = C_1 - SK_i^T\boldsymbol{y} (\bmod q)$；令 $m = (m_1, m_2, \ldots, m_m)$，如果 m_i 与 $\left\lfloor \frac{q}{2} \right\rfloor$ 相比更接近 0，则 $m_i = 0$；否则，$m_i = 1$；输出 $m = (m_1, m_2, \ldots, m_m)$。

(7)一级解密 $\text{Dec}_1(params, SK_j, C_j)$：输入 SK_j 和一级密文 C_j，计算 $m = C_1' - SK_j^T\boldsymbol{y} (\bmod q)$；令 $m = (m_1, m_2, \ldots, m_m)$，如果 m_i 与 $\left\lfloor \frac{q}{2} \right\rfloor$ 相比更接近 0，则 $m_i = 0$；否则，$m_i = 1$；输出 $m = (m_1, m_2, \ldots, m_m)$。

(8)问责算法 $\text{Judge}^{D_{i,\mu}}(params, id_i, id_p)$：提供一个解密设备 $D_{i,\mu}$ 作为预言机：

1)重复下面的实验 $n = \lambda / \mu$ 次。选择均匀随机向量 $s \in \mathbb{Z}_q^n$ 和明文 m，并且计算 $C_1 = (\boldsymbol{U}_i^T + \boldsymbol{U}_p^T)\boldsymbol{s} + m\left\lfloor \frac{q}{2} \right\rfloor + \boldsymbol{e}$，$\boldsymbol{y} = \boldsymbol{A}^T\boldsymbol{s} + \boldsymbol{e}$，密文 $C = (C_1, \boldsymbol{y})$；运行解密设备 $D_{i,\mu}$，并将 C 作为 $D_{i,\mu}$ 的输入，输出 m'；

2)如果 $m' = m$，输出“Proxy”并退出；否则输出“Delegator”。

3.2　正确性

(1)　二级密文解密 $\text{Dec}_2(params, SK_i, C_i)$

$$\begin{aligned} m &= C_1 - SK_i^T\boldsymbol{y} (\bmod q) \\ &= \boldsymbol{U}_i^T\boldsymbol{s} + m\left\lfloor \frac{q}{2} \right\rfloor + \boldsymbol{e} - \boldsymbol{X}_i^T(\boldsymbol{A}^T\boldsymbol{s} + \boldsymbol{e}) (\bmod q) \end{aligned}$$

$$=\boldsymbol{U}_i^T\boldsymbol{s}+m\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}-\boldsymbol{U}_i^T\boldsymbol{s}-\boldsymbol{X}_i^T\boldsymbol{e}(\bmod q)$$
$$=\boldsymbol{e}-\boldsymbol{X}_i^T\boldsymbol{e}+m\left\lfloor\frac{q}{2}\right\rfloor(\bmod q)$$

因为 $\boldsymbol{e}$ 和 SK_i^T 是从高斯分布的集合 ψ_s 中选择的，所以在 $s=\alpha_q$ 时，$\boldsymbol{e}-\boldsymbol{X}_i^T\boldsymbol{e}$ 小于 $\left\lfloor\frac{q}{4}\right\rfloor$，成功恢复 m。

(2)一级密文解密 $\mathrm{Dec}_1(params,SK_j,C_j)$

$$C_1^{'}=C_1+rk_{i\to j}-SK_p^T\boldsymbol{y}+\boldsymbol{e_2}$$
$$=\boldsymbol{U}_i^T\boldsymbol{s}+m\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}+(\boldsymbol{U}_j^T-\boldsymbol{U}_i^T+\boldsymbol{U}_p^T)\boldsymbol{s}+\boldsymbol{e_1}-\boldsymbol{X}_p^T\boldsymbol{y}+\boldsymbol{e_2}$$
$$=\boldsymbol{U}_j^T\boldsymbol{s}+\boldsymbol{e}+\boldsymbol{e_1}-\boldsymbol{X}_p^T\boldsymbol{e}+\boldsymbol{e_2}+m\left\lfloor\frac{q}{2}\right\rfloor$$

$$m=C_1^{'}-C_2^{'}-SK_j^T\boldsymbol{y}(\bmod q)$$
$$=\boldsymbol{U}_j^T\boldsymbol{s}+\boldsymbol{e}+\boldsymbol{e_1}-\boldsymbol{X}_p^T\boldsymbol{e}+\boldsymbol{e_2}+m\left\lfloor\frac{q}{2}\right\rfloor-\boldsymbol{X}_j^T(\boldsymbol{A}^T\boldsymbol{s}+\boldsymbol{e})(\bmod q)$$
$$=\boldsymbol{e}+\boldsymbol{e_1}-\boldsymbol{X}_j^T\boldsymbol{e}-\boldsymbol{X}_p^T\boldsymbol{e}+\boldsymbol{e_2}+m\left\lfloor\frac{q}{2}\right\rfloor(\bmod q)$$

因为 $\boldsymbol{e}$，$\boldsymbol{e_1}$，$\boldsymbol{e_2}$，SK_j^T，$SK_p{}^T$ 是从高斯分布的集合 ψ_s 中选择的，所以在 $s=\alpha_q$ 时，$\boldsymbol{e}+\boldsymbol{e_1}-\boldsymbol{X}_j^T\boldsymbol{e}-\boldsymbol{X}_p^T\boldsymbol{e}+\boldsymbol{e_2}$ 小于 $\left\lfloor\frac{q}{4}\right\rfloor$，成功恢复 m。

3.3　多跳性

代理者执行第一次重加密：

$$C_2=C_1+rk_{1\to 2}-SK_p^T\boldsymbol{y}+\boldsymbol{e_2}$$

代理者执行第二次重加密：

$$C_3=C_2+rk_{2\to 3}-SK_p^T\boldsymbol{y}+\boldsymbol{e_2}$$
$$=C_1+rk_{1\to 2}+rk_{2\to 3}-2SK_p^T\boldsymbol{y}+2\boldsymbol{e_2}$$

代理者执行第 N-1 次重加密：

$$C_N=C_{N-1}+rk_{N-1\to N}-SK_p^T\boldsymbol{y}+\boldsymbol{e_2}$$
$$=C_{N-2}+rk_{N-2\to N-1}+rk_{N-1\to N}-2SK_p^T\boldsymbol{y}+2\boldsymbol{e_2}=\ldots$$
$$=C_1+\sum_{i=1}^{N-1}rk_{i\to i+1}-(N-1)SK_p^T\boldsymbol{y}+(N-1)\boldsymbol{e_2}$$
$$=C_1+\sum_{i=1}^{N-1}((\boldsymbol{U}_{i+1}^T-\boldsymbol{U}_i^T+\boldsymbol{U}_p^T)\boldsymbol{s}+\boldsymbol{e_1})-(N-1)\boldsymbol{X}_p^T\boldsymbol{y}+(N-1)\boldsymbol{e_2}$$
$$=\boldsymbol{U}_1^T\boldsymbol{s}+m\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}+(-\boldsymbol{U}_1^T+\boldsymbol{U}_N^T)\boldsymbol{s}+(N-1)\boldsymbol{e_1}-(N-1)\boldsymbol{X}_p^T\boldsymbol{e}+(N-1)\boldsymbol{e_2}$$
$$=m\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}+\boldsymbol{U}_N^T\boldsymbol{s}+(N-1)\boldsymbol{e_1}-(N-1)\boldsymbol{X}_p^T\boldsymbol{e}+(N-1)\boldsymbol{e_2}$$

完成 N-1 次重加密后，使用用户 N 的私钥 SK_N 完成解密：

$$m=C_N-SK_N^T\boldsymbol{y}(\bmod q)$$
$$=m\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}+\boldsymbol{U}_N^T\boldsymbol{s}+(N-1)\boldsymbol{e_1}-(N-1)\boldsymbol{X}_p^T\boldsymbol{e}+(N-1)\boldsymbol{e_2}-$$
$$\boldsymbol{X}_N^T(\boldsymbol{A}^T\boldsymbol{s}+\boldsymbol{e})(\bmod q)$$
$$=m\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}+(N-1)\boldsymbol{e_1}-(N-1)\boldsymbol{X}_p^T\boldsymbol{e}+(N-1)\boldsymbol{e_2}-\boldsymbol{X}_N^T\boldsymbol{e}(\bmod q)$$

当 $\boldsymbol{e}+(N-1)\boldsymbol{e_1}-(N-1)\boldsymbol{X}_p^T\boldsymbol{e}+(N-1)\boldsymbol{e_2}-\boldsymbol{X}_N^T\boldsymbol{e}$ 小于 $\left\lfloor\frac{q}{4}\right\rfloor$ 时，成功恢复 m。

4　安全性与效率分析

4.1　CPA 安全

定理 4.1　令 λ 为安全参数，对于任意明文 $m\in\{0,1\}$，若 LWE 问题在多项式时间是不可解的，则该方案满足 IND-aID-CPA 安全。即敌手$\mathcal{A}$在多项式时间 t 内成功攻破方案的优势 $\mathrm{ADV}_{\mathrm{PRE},\mathcal{A}}^{\mathrm{IND\text{-}CPA}}(t)\le negl(\lambda)$。

证明：　通过证明下列游戏的不可区分性来证明 PPT 敌手$\mathcal{A}$成功攻破方案的优势是可忽略的。

游戏 1　原始的 IND-aID-CPA 方案。在挑战阶段，当挑战者$\mathcal{C}$收到 (i^*,m_0,m_1) 后，挑选其中一个明文 m_b，计算挑战密文 $C^*=(C_1,\boldsymbol{y})$ 给敌手$\mathcal{A}$，其中 $C_1=\boldsymbol{U}_i^T\boldsymbol{s}+m_b\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}$，$\boldsymbol{y}=\boldsymbol{A}^T\boldsymbol{s}+\boldsymbol{e}$。最后，敌手$\mathcal{A}$猜测 $b^{'}$，若猜测成功，则$\mathcal{C}$输出 1，否则输出 0。

游戏 2　在游戏 2 中矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 与矩阵 $\boldsymbol{U_0},\boldsymbol{U_1},\ldots,\boldsymbol{U_m}\in\mathbb{Z}_q^{n\times m}$ 的生成方式与游戏 1 不同。在游戏 2 中，挑战者$\mathcal{C}$模拟真实的方案，并回答敌手$\mathcal{A}$的各种问询。首先挑战者模拟真实方案如下：

初始阶段：挑战者$\mathcal{C}$选择一个随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，根据以下步骤生成 $\boldsymbol{U_0},\boldsymbol{U_1},\ldots,\boldsymbol{U_m}\in\mathbb{Z}_q^{n\times m}$：

1)挑战者$\mathcal{C}$随机选择服从高斯分布 $D_{\sigma/(m+1),0}$ 的 m+1 个矩阵 $\boldsymbol{X_0},\boldsymbol{X_1},\ldots,\boldsymbol{X_m}$；

2)计算 $\boldsymbol{AX_k}=\boldsymbol{U_k}\bmod q$，$k=0,1,\ldots,m$；

3)若生成的矩阵 $\boldsymbol{U_k}$ 是线性相关的，则重新选择生成 $\boldsymbol{X_k}$。

挑战者$\mathcal{C}$将公共参数 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{U_0},\boldsymbol{U_1},\ldots,\boldsymbol{U_m}\in\mathbb{Z}_q^{n\times m}$ 发送给敌手$\mathcal{A}$。

阶段 1：敌手$\mathcal{A}$可以进行下面一系列的问询过程，挑战者回答敌手$\mathcal{A}$下列问询：

(1)代理密钥问询：代理商的私钥 $\boldsymbol{X_p}\in\mathbb{Z}_q^{m\times m}$ 是由挑战者$\mathcal{C}$均匀随机选择的小范数矩阵，计算 $\boldsymbol{AX_p}=\boldsymbol{U_p}$，将代理商的私钥对 SK_p 发送给$\mathcal{A}$；

(2)密钥提取问询：敌手$\mathcal{A}$发送用户身份 id 给挑战者$\mathcal{C}$，$\mathcal{C}$计算 $\boldsymbol{X}=\boldsymbol{X_0}+\sum_{i=1}^{m}id_i\boldsymbol{X_i}$，所以 $\boldsymbol{AX}=\boldsymbol{U}=\boldsymbol{U_0}+\sum_{i=1}^{m}id_i\boldsymbol{U_i}(\bmod q)$。最后，$\mathcal{C}$将 $\boldsymbol{X}=\boldsymbol{X_0}+\sum_{i=1}^{m}id_i\boldsymbol{X_i}$ 发送给$\mathcal{A}$作为用户私钥；

(3)重加密密钥问询：敌手$\mathcal{A}$发送身份集 (id_i,id_j,id_p) 给挑战者$\mathcal{C}$，挑战者$\mathcal{C}$按照上面的步骤计算生成 $\boldsymbol{U_i}$，$\boldsymbol{U_j}$ 和 $\boldsymbol{U_p}$，然后，使用计算好的公钥计算生成重密钥 $rk_{i\to j}=(\boldsymbol{U}_j^T-\boldsymbol{U}_i^T+\boldsymbol{U}_p^T)\boldsymbol{s}+\boldsymbol{e_1}$，并发送给$\mathcal{A}$。

阶段 2(挑战阶段)：当挑战者$\mathcal{C}$收到来自敌手$\mathcal{A}$的 id^*,m_0,m_1。挑战者随机选择 $b\in\{0,1\}$，计算 $C=\boldsymbol{U}_{id^*}^T\boldsymbol{s}+m_b\left\lfloor\frac{q}{2}\right\rfloor+\boldsymbol{e}$，$\boldsymbol{y}=\boldsymbol{A}^T\boldsymbol{s}+\boldsymbol{e}$，并发送 $C^*=(C,\boldsymbol{y})$ 给敌手。最后敌手$\mathcal{A}$猜测 b'，如果 $b'=b$，则挑战者$\mathcal{C}$输出 1，否则输出 0。

游戏 3　在游戏 2 中，通过加密算法计算生成挑战密文 C^*。在游戏 3 中，直接从 $\mathbb{Z}_q^m\times\mathbb{Z}_q^m$ 中随机选择 C^*。显然，敌手$\mathcal{A}$在游戏 3 中可获得的优势为 0。

通过将问题规约到 LWE 难题来证明两个游戏的不可区分性。若敌手$\mathcal{A}$能够区分两个游戏的优势为 ε，则使用下面的算法 B 能够攻破 LWE 困难问题[12]。

算法 B　收到了随机实例 $(\boldsymbol{a_i},y_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$，其中 $y_i=\boldsymbol{a}_i^T\boldsymbol{s}+\boldsymbol{e_i}$，$\boldsymbol{A}=(\boldsymbol{a_1},\boldsymbol{a_2},\ldots,\boldsymbol{a_m})$，$\boldsymbol{y}=(y_1,y_2,\ldots,y_m)$。计算：

$$C^*=\boldsymbol{X}^T\boldsymbol{y}+m\left\lfloor\frac{q}{2}\right\rfloor$$
$$=\boldsymbol{X}^T(\boldsymbol{A}^T\boldsymbol{s}+\boldsymbol{e})+m\left\lfloor\frac{q}{2}\right\rfloor$$
$$=\boldsymbol{U}^T\boldsymbol{s}+\boldsymbol{e}+m\left\lfloor\frac{q}{2}\right\rfloor$$

若敌手$\mathcal{A}$成功猜测出 m，则算法 B 输出 1，否则输出 0。

如果 y 选取的是均匀随机的向量，则 C^* 也是均匀随机的，敌手$\mathcal{A}$以不超过 $1/2$ 的概率成功猜测出 m。

若 y 是由 $\boldsymbol{y}=\boldsymbol{A}^T\boldsymbol{s}+\boldsymbol{e}$ 产生的，则 C^* 也是均匀分布的。此时敌手$\mathcal{A}$有 $(1+\varepsilon)/2$ 的优势猜测出 m，算法 B 同样有 $(1+\varepsilon)/2$ 的概率输出 1。即算法 B 有 $\varepsilon/2$ 的优势解决 LWE 问题。但是，LWE 为格上难题，算法 B 不能求解出 LWE 困难问题，所以 $\varepsilon/2$ 的优势是可忽略的。

显然，游戏 2 和游戏 3 是不可区分的。因此，敌手$\mathcal{A}$在游戏 2 中的可以取得优势也为 0。

同样地，对于任意 PPT 敌手$\mathcal{A}$来说，游戏 1 和游戏 2 也是不可区分的。由于矩阵 A 是随机的，且 $\boldsymbol{U_i}$ 服从高斯分布，

根据定理 3，$AX_i = U_i \bmod q$ 上的分布与 $\mathbb{Z}_q^{n\times m}$ 上的均匀分布在统计量上是接近的，故无法区分游戏 1 和 2。因此，敌手$\mathcal{A}$在游戏 1 中获得的优势也为 0。

综上所述，在标准模型下，APRE 方案满足 IND-aID-CPA 安全性。

4.2 可问责性

为了证明方案的可问责性，本文将证明方案满足恶意代理安全和恶意授权者安全。

4.2.1 恶意代理安全

定理 4.2 在 LWE 困难问题下，若敌手$\mathcal{A}$在多项式时间 t 内成功诬陷授权者的优势 $\mathrm{ADV}_{\mathrm{PRE},\mathcal{A}}^{\mathrm{mp}}(t) \le negl(\lambda)$，则方案满足恶意代理安全，即敌手$\mathcal{A}$输出一个解密算法，使审判算法输出"Delegator"的优势是可忽略的。

证明 为了证明方案是恶意代理安全的，本文提出以下两个实验，通过证明两个实验的不可区分性和在实验 Exp_1 中敌手$\mathcal{A}$的优势是可忽略的完成恶意代理安全的证明。

实验 Exp_0　原始恶意代理安全实验。敌手$\mathcal{A}$输出一个能够以不可忽略的概率 μ 获得明文的解密设备 $D_{*,\mu}$，挑战者$\mathcal{C}$用 n 个不规则明文作为输入运行解密设备 $D_{*,\mu}$。不规则密文为 $C_1 = (U_i^T + U_p^T)s + m\left\lfloor \frac{q}{2} \right\rfloor + e$，$y = A^T s + e$，其中 $s \leftarrow \mathbb{Z}_q^n$。

实验 Exp_1　原始恶意代理安全对比实验。与 Exp_0 的不同在于不规则密文，Exp_1 中密文为 $C_1 = U_i^T s + m\left\lfloor \frac{q}{2} \right\rfloor + e$，$y = A^T s + e$，其中 $s \leftarrow \mathbb{Z}_q^n$。

接下来使用引理 4.1 和引理 4.2 证明以上两个实验在计算上的不可区分性，且在实验 Exp_1 中敌手成功诬陷授权者的概率可忽略。

引理 4.1 基于 LWE 困难问题假设下，Exp_1 与 Exp_0 在计算上是不可区分的。

按照游戏 2 中的步骤生成 $U_0, U_1, \ldots, U_m$，可知 $AX_i = U_i \bmod q$ 的分布与 $\mathbb{Z}_q^{n\times m}$ 上均匀分布的统计量相近。

敌手$\mathcal{A}$输出一个解密设备 $D_{i,\mu}$，挑战者$\mathcal{C}$运行审判算法 $\mathrm{Judge}^{D_{i,\mu}}$：

1)重复以下实验 $\mathrm{n} = \lambda / \mu$ 次。均匀随机的选择向量 $s \in \mathbb{Z}_q^n$，$r \in \mathbb{Z}_q^n$ 和明文 m，计算 $C_1 = U_i^T s + r + m\left\lfloor \frac{q}{2} \right\rfloor + e$，$y = A^T s + e$，密文 $C = (C_1, y)$；运行解密设备 $D_{i,\mu}$，并将 C 作为 $D_{i,\mu}$ 的输入，输出 m'；

2)如果 $m' = m$，输出"Proxy"并退出；否则输出"Delegator"。

对于上述审判算法，若 $r = e$，则 $C_1 = (U_i^T + U_p^T)s + m\left\lfloor \frac{q}{2} \right\rfloor + 2e$，此时$\mathcal{C}$成功模拟实验 Exp_0；若 $r = -X_p^T y$，则 $C_1 = U_i^T s + m\left\lfloor \frac{q}{2} \right\rfloor + (e - X_p^T e)$，此时$\mathcal{C}$成功模拟实验 Exp_1；由于 e 和 X_p 均服从高斯分布，故对于$\mathcal{A}$是不可区分的。即实验 Exp_1 与 Exp_0 在计算上是不可区分的。

引理 4.2 在 Exp_1 中敌手$\mathcal{A}$输出一个解密设备，使得审判算法输出"Delegator"的优势可以忽略。

在一次实验中，由于 Exp_1 解密设备的输入密文 $C_1 = (U_i^T + U_p^T)s + m\left\lfloor \frac{q}{2} \right\rfloor + e$，$y = A^T s + e$，为普通密文，所以 $D_{i,\mu}$ 将以 μ 的概率返回明文 $m' = m$，则敌手$\mathcal{A}$在 Exp_1 中的优势为 $(1-\mu)^n = (1-\mu)^{\lambda/\mu} \le \frac{1}{e^\lambda}$，故敌手的优势是可忽略的。

4.2.2 恶意授权者安全

定理 4.3 在 LWE 困难假设下，若敌手$\mathcal{A}$在多项式时间 t 内成功诬陷代理商的优势 $\mathrm{ADV}_{\mathrm{PRE},\mathcal{A}}^{\mathrm{md}}(t) \le negl(\lambda)$，则方案满足恶意代理安全，即敌手$\mathcal{A}$输出一个解密算法，使审判算法输出"Proxy"的优势是可忽略的。

证明 为了证明方案是恶意授权者安全的，提出以下两个实验，通过证明两个实验的不可区分性和在实验 Exp_1 中敌手$\mathcal{A}$的优势是可忽略的完成恶意授权者安全的证明。

实验 Exp_0　原始恶意授权者安全实验。当敌手$\mathcal{A}$输出一个能够以不可忽略的概率 μ 获得明文的解密设备 $D_{i,\mu}$，挑战者$\mathcal{C}$用 n 个不规则明文作为输入运行解密设备 $D_{i,\mu}$。不规则密文为 $C_1 = (U_i^T + U_p^T)s + m\left\lfloor \frac{q}{2} \right\rfloor + e$，$y = A^T s + e$，其中 $s \leftarrow \mathbb{Z}_q^n$。

实验 Exp_1　原始恶意授权者安全对比实验。与 Exp_0 不同是审判算法的输入密文不同。均匀随机的选择矩阵 $R \in \mathbb{Z}_q^{n\times m}$，密文为 $C_1 = (U_i^T + R^T)s + m\left\lfloor \frac{q}{2} \right\rfloor + e$，$y = A^T s + e$，其中 $s \leftarrow \mathbb{Z}_q^n$。

接下来使用引理 4.3 和引理 4.4 证明以上两个实验在计算上的不可区分性，且在实验 Exp_1 中敌手成功诬陷代理商的概率可忽略。

引理 4.3 基于 LWE 困难问题假设下，Exp_1 与 Exp_0 在计算上是不可区分的。

使用游戏 2 中的方式生成 $U_0, U_1, \ldots, U_m$，可知 $AX_i = U_i \bmod q$ 的分布与 $\mathbb{Z}_q^{n\times m}$ 上的均匀分布在统计量上相近，故得证。

引理 4.4 在 Exp_1 中敌手输出一个解密设备，使审判算法输出"Proxy"的优势是可忽略的。

解密设备 $D_{i,\mu}$ 的输入密文为 $C_1 = (U_i^T + R^T)s + m\left\lfloor \frac{q}{2} \right\rfloor + e$，$y = A^T s + e$。由于 R 是均匀随机的，$D_{i,\mu}$ 输出 $m' = m$ 的概率为 $1/|M| = \frac{1}{2^m}$。根据二级解密算法可知，解密结果为 $R^T s + e - X_i^T e + m\left\lfloor \frac{q}{2} \right\rfloor$。因为 R 是均匀随机的，无法恢复出明文 m；且 $(\frac{1}{|M|})^n < \frac{1}{2^m}$，可知敌手$\mathcal{A}$在 Exp_1 的优势是可忽略的。

4.3 效率分析

文献[13]中提出的可问责代理重加密基于 DBDH 困难假设，计算复杂度较高且存在证书管理问题。文献[20]中提出了格上基于身份的 PRE 方案，该方案可以加密多比特信息，但是方案是交互式的，被授权者需要提供自己的私钥来生成重密钥，容易造成密钥泄露的问题。文献[21]中提出单跳的格上 PRE 方案，使用陷门生成私钥。本文所提方案完成了可问责性和抗合谋攻击的设计；具有单向性和多跳性，密文扩展性良好；能够抵抗量子攻击。表 1 给出了文献[13]、[20]与本方案的存储空间和性能上的对比。其中，$|\mathbb{G}|$ 是群 $\mathbb{G}$ 中元素的个数，$|\mathbb{G}_T|$ 表示 $\mathbb{G}$ 中元素的位长，$\log q$ 表示 $\log_2 q$。表 2 选择文献[20]、[21]与本方案的三个格上代理重加密方案进行计算和通信复杂度对比，其中，密文开销指 1bit 明文对应的密文大小，MMM 为矩阵间乘法，MMA 为矩阵间加法，VMM 为向量矩阵乘法，VCM 为常数向量乘法，VVM 为向量间加法，EGT 为群 $\mathbb{G}_T$ 中的幂运算，EG 为群 $\mathbb{G}$ 中的幂运算。

表 1　存储空间和性能比较

Tab. 1　Comparison of storage space and performance

方案	私钥尺寸	单向性	困难问题	IBE	可问责性
文献[13]	$2\|\mathbb{G}\|$	是	DBDH	否	是
文献[20]	$O(ml\log q)$	否	LWE	是	否
文献[21]	$O(n^2 k\log q)$	是	LWE	否	否
本文方案	$O(mn\log q)$	是	LWE	是	是

结合两个表格的比较结果，本文方案在私钥尺寸上优于文献[21]，并且相较于其他方案满足单向性和可问责性；计算复杂度低于文献[20]，且密钥开销与文献[13]、[21]相比较低。因此，本文方案较为良好的安全性和较高的效率。

表 2　计算和通信复杂度比较

Tab. 2　Comparison of computational and communication complexity

方案	计算复杂度	密文开销
文献[13]	2EGT+2EG	$\frac{2\|\mathbb{G}_T\|+2\|\mathbb{G}\|}{\|\mathbb{G}\|}$
文献[20]	2VMM+2VCM+3VVA	2
文献[21]	2MMM+2MMA+1VMM	$\frac{n^2+n\log n}{n\log n}$
本文方案	2VMM+1VCM+3VVA	2

5　结束语

本文提出了一个格上基于身份的可问责代理重加密方案。在方案中，用户的身份被计算为一个矩阵作为公钥，提高了私钥提取的效率；重密钥由用户公钥计算生成，具有非交互性；使用公共问责算法抑制恶意代理商滥用重密钥的行为。该方案具有单向性和多跳性等性质。安全分析表明，方案满足标准模型下的 IND-aID-CPA 安全；效率分析则说明了方案在存储空间和性能方案较有优势。但是方案在计算效率上还有一定的优化空间，构造更加高效的格上可问责的代理重加密的方案也是未来的研究方向。

参考文献：

[1] Blaze M, Bleumer G, Strauss M, *et al.* Divertible protocols and atomic proxy cryptography [C]// Theory and Application of Cryptographic Techniques, 1998: 127-144

[2] Green M, Ateniese G. Identity-Based Proxy Re-encryption [C]// applied cryptography and network security, 2007: 288-306.

[3] Xagawa K. Cryptography with Lattices [D]. [Ph. D. dissertation] , Tokyo Institute of Technology, 2010. http://xagawa. net/pdf/2010Thesis. pdf.

[4] Singh K, Rangan C P, Banerjee A K. Lattice-based identity based unidirectional proxy re-encryption scheme [C]// International Conference on Security, Privacy, and Applied Cryptography Engineering, Pune, India, 2014: 76–91.

[5] 汤永利, 刘琦, 张晓航, 等. 格上基于RLWE难题的身份基代理重加密方案 [J]. 计算机应用研究, 2021, 38 (04): 1199-1202. (Tang Yongli, Liu Qi, Zhang Xiaohang, *et al.* Identity-based proxy re-encryption scheme based on RLWE problem [J]. Application Research of Computers, 2021, 38 (04): 1199-1202.)

[6] Kim K S, Jeong I R. Collusion-resistant unidirectional proxy re-encryption scheme from lattices [J]. Journal of Communications and Networks, 2016: 1-7.

[7] Wang X Y, Hu A Q, Hao F. Improved collusion-resistant unidirectional proxy re-encryption scheme from lattice [J]. IET Information Security, 2020: 342-351.

[8] Dutta P, Susilo W, Duong D H, *et al.* Collusion-Resistant Identity-based Proxy Re-Encryption: Lattice-based Constructions in Standard Model [J]. Theoretical Computer Science, vol. 871, 2021: 16-29.

[9] Wang X A, Ge Y, Yang X. PRE+: Dual of proxy re-encryption and its application [C]// Cryptology ePrint Archive, 2013.

[10] Singh K, Rangan C P, Agrawal R, *et al.* Provably secure lattice based identity based unidirectional PRE and PRE+schemes [J]. Journal of Information Security and Applications, 2020, 54 (3/4): 102569.

[11] Ateniese G, Fu K, Green M, *et al.* Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage [J]. ACM Transactions on Information and System Security, vol. 9, no. 1, 2006: 1-30.

[12] Guo H, Zhang Z F, Xu J, *et al.* Non-Transferable Proxy Re-Encryption [J]. The Computer Journal, vol. 62, no. 4, 2019: 490-506.

[13] Guo H, Zhang Z F, Xu J, *et al.* Accountable Proxy Re-Encryption for Secure Data Sharing [J]. IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, 2021: 145-159.

[14] Ajtai M. Generating hard instances of lattice problems [C]// The 28th ACM Symposium on Theory of Computing. New York: ACM, 1996: 99-108.

[15] Gentry C, Peikert C, Vaikuntanathan V. How to use a short basis: Trapdoors for hard lattices and new cryptographic constructions [C]// The 40th ACM Symposium on Theory of Computing, Victoria, Canada, 2008: 197–206.

[16] 王凤和, 胡予濮, 贾艳艳. 标准模型下的格基数字签名方案 [J]. 西安电子科技大学学报, 2012, 39 (04): 57-61, 119. (Wang Fenghe, Hu Yupu, Jia Yanyan. Lattice-based signature scheme in the standard model [J]. Journal of Xidian University, 2012, 39 (04): 57-61, 119.)

[17] Micciancio, D, Peikert C. Hardness of SIS and LWE with Small Parameters [C]// The 33rd Annual International Cryptology Conference, vol. 2013: 21-39.

[18] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography [C]// Proceedings of the 37th annual ACM symposium on Theory of computing. ACM, 2005: 84-93.

[19] Wang X Y, Hu A Q, Hao F. Feasibility Analysis of Lattice-Based Proxy Re-Encryption [C]// Proc of the 17th International Conference on Cryptography, Security and Privacy, 2017: 12-16.

[20] Hou J, Jiang M, Guo Y, *et al.* Efficient identity-based multi-bit proxy re-encryption over lattice in the standard model [J]. Information Security Technical Report, 2019: 329-334.

[21] Kirshanova E. Proxy re-Encryption from lattices [C]// Proc of the 17th International Conference on Public-Key Cryptography Volume 8383, 2014: 77-94.